ITRI 615

Pfleeger Chapter 2 & 12

Whitman & Mattord Chapter 8

Cryptography terminology

- Encryption is the process of encoding a message so that its meaning is not obvious. Also referred to as encode or encipher.
- Decryption is the reverse process. Also referred to as decode or decipher.
- Cryptosystem is a system for encryption and decryption.
- The original form of a message is called plaintext, and the encrypted form is called cyphertext.
- Symmetric encryption uses the same key for encryption and decryption, whereas asymmetric encryption uses a different key for encryption and decryption.

Cryptanalysis (breaking the code)

- A cryptanalyst can attempt to do any or all of six different things:

1. Break a single message.
2. Recognize patterns in encrypted messages, to be able to break subsequent ones.
3. Infer some meaning without even breaking the encryption.
4. Deduce the key, to break subsequent messages easily.
5. Find weaknesses in the implementation or environment of use of encryption.
6. Find general weaknesses in an encryption algorithm.

An algorithm might be theoretically breakable, but impractical to break.

Substitution ciphers

- Caesar cipher is the most well known, as it was first used by Julius Caesar himself.

- A scheme whereby each letter is translated to the letter a fixed number of places after it in the alphabet.

- For example, a Caesar cipher, with a shift of 4 to the right:

  Plaintext: H E L L O
  Ciphertext: L I P P S

- Advantageous that it is quite simple, disadvantage is its obvious pattern.

A secure encryption algorithm

- In 1949 Claude Shannon proposed several characteristics that identify a good cipher.

1. The amount of secrecy needed should determine the amount of labor that's appropriate.
2. The set of keys and algorithm should be free from complexity.
3. The implementation of the process should be as simple as possible.
4. Errors in ciphering should not propagate and cause corruption of further information.
5. The size of the enciphered text should be no larger than that of the original text.

DES (Data Encryption Standard)

- Based on substitution (confusion) and transposition (diffusion).
- Plaintext is encrypted in blocks of 64 bits, and the key can be any 56 bit number, as the extra 8 bits are check digits and do not affect the encryption.
- The user can change the key at any time.
- The plaintext is affected by a series of cycles of a substitution then a permutation.
- Although complex, it is repetitive, thereby making it suitable for implementation on a single-purpose chip (see p. 97 table 2.11).

AES (Advanced Encryption Standard)

- Encryption takes place in blocks of 128 bits.

- Like DES, AES uses repeat cycles.

- 10, 12 or 14 cycles for keys of 128, 192 and 256 bits respectively.

- Each cycle consists of 4 steps (see p. 74 figure 2.9):

1. Byte substitution, according to a substitution table.
2. Shift row, where rows and bytes are shifted depending on key size.
3. Mix column.
4. Add subkey, where a portion of the key is included with the cycle result.

Being new is its major strength.

DES vs AES

- Both DES and AES are examples of symmetrical (secret) key encryption. With secret key the encrypter and the decrypter must have access to the same key to enable communication.

- See table 2.12 on page 100 for a direct comparison between DES and AES.

Public key encryption

- With public key encryption each user has a key that does not have to be kept secret.
- The public nature of the key does not compromise the secrecy of the system.
- The key is therefore divulged, but the trick is to keep the decryption technique secret.
- This goal is accomplished by using two keys, one for encryption and another for decryption.
- See page 104 table 2.13 for a comparison between secret key and public key encryption.

Merkle-Hellman Knapsacks

- The knapsack problem presents a set of positive integers and a target sum, with the goal of finding a subset of the integers that sum to the target.

- Idea is to encode a binary message as a solution to a knapsack problem, reducing the ciphertext to the target sum obtained by adding terms corresponding to 1's in the plaintext.

- The algorithm begins with a knapsack filled with pre-determined values. The plaintext is mapped to these values, where order is extremely important. The values aligned to 1's in the plaintext, are added together to form the target sum.

- The target sum is needed for the decryption, as each set of values in the knapsack sum to a unique target sum.

RSA (Rivest-Shamir-Adelman)

- RSA relies on number theory, where properties of numbers such as their prime factors are studied. Similar to Merkle-Hellman in finding terms that add to a particular sum or multiply to a particular product.

- The algorithm combines results from number theory with the degree of difficulty in determining the prime factors of a given number.

- Based on the underlying problem of factoring large numbers.

- Plaintext block P is encrypted by P^e mod n, with e being the encryption algorithm, and n being a factor chosen as part of the key.

- P is decrypted by $(C^e)^d$ mod n, with C being the ciphertext, and d being the decryption algorithm.

Key exchange

- Used when protected data needs to be sent to someone you don't know and who also doesn't know you. For example e-filing, you don't know who will receive it at SARS and they also don't know you.

- The solution is for the sender to send the receiver:

$$E(k_{PUB\text{-}R}, E(k_{PRIV\text{-}S},K))$$

where k is the key, both receiver public and private sender, K is the symmetric key, and E is the encryption algorithm (see fig 2.11 p.81).

- The protocol therefore adds two layers of protection, the first is unwrapped with the senders public key, and the second with receivers private key.

Digital signatures

- A protocol that produces the same effect as a real signature.
- A mark that only the sender can make, but other can easily recognize as belonging to the sender.
- A need was realized when money started to be transacted electronically.
- Properties include:

1. It must be unforgeable.
2. It must be authentic.
3. It is not alterable.
4. It is not reusable.

Hash functions

- Mathematical algorithms that generate a message summary or digest to confirm the identity of a specific message and to confirm that there haven't been any changes to the content.

- Created by converting variable-length messages into a single fixed-length value.

- Hash values are computed at the sending and receiving side. These values are compared, and if equal, message transmission has been successful without alteration.

- A hash function will always provide the same hash value for the same message, and the hash value cannot be used to determine message contents.

Questions

- Any questions?